Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WT Docket No. 16-106
Broadband and Other Telecommunications	)	
Services	)	

REPLY COMMENTS OF THE INTERNET ASSOCIATION

Mark W. Brennan
Partner
Hogan Lovells US LLP
555 13th Street, NW
Washington, DC 20004
(202) 637-6409

Abigail Slater
General Counsel
The Internet Association
1333 H Street NW
West Tower, Floor 12
Washington, DC 20005
(202) 770-0023

Counsel for The Internet Association

July 6, 2016

TABLE OF CONTENTS

Page

I. INTRODUCTION. 1

II. A DIVERSE ARRAY OF COMMENTERS SUPPORT THE COMMISSION'S PROPOSED FINDING THAT SECTION 222 DOES NOT APPLY TO PROVIDERS OF EDGE SERVICES AND OTHER NON-TITLE II OFFERINGS. 2

III. EDGE PROVIDERS DO NOT HAVE THE SAME ACCESS TO CONSUMER INFORMATION AS BIAS PROVIDERS. 5

A. Edge Providers Have More Limited Visibility Into Online Practices And Consumer Information. 5

B. Encryption Provides Additional Privacy Protections But Does Not Negate BIAS Providers' Access to Consumer Data. 7

C. Market Entry Challenges And Switching Costs May Limit BIAS Customers' Data Privacy And Security Choices. 9

IV. THE FTC'S FLEXIBLE APPROACH TO DATA PRIVACY AND SECURITY ENFORCEMENT CAN BETTER PROTECT CONSUMERS AND ENCOURAGE INNOVATION THAN A HOST OF PRESCRIPTIVE RULES. 12

V. THE FCC SHOULD THOUGHTFULLY ADDRESS OTHER FTC BUREAU STAFF PROPOSALS 15

VI. CONCLUSION. 17

EXECUTIVE SUMMARY

A diverse array of commenters agree that the Federal Communications Commission ("FCC" or "Commission") could not and should not apply Section 222 of the Communications Act to providers of "edge" services. Adopting additional data privacy and security requirements for edge services and non-Title II offerings would upend the current regulatory framework for those services without providing meaningful additional benefits for consumers. And while some commenters urge the Commission not to create different regulatory environments between BIAS providers and edge providers (and may be implying that the proposed rules should also apply to edge providers), these parties utterly fail to identify sufficient legal authority or need for the FCC to extend new requirements to edge services.

Edge providers allow consumers to explore, engage, consume, connect, and create on the Internet with a multitude of choices. Contrary to suggestions from some commenters, edge providers do not have access to more or a wider range of user information than BIAS providers. Edge providers only typically have direct access to information that consumers voluntarily choose to provide, and they tend to offer granular privacy settings that give consumers significant control over their personal information. In contrast, BIAS providers serve as the gateway to the Internet, which provides them access to potentially all of their subscribers' Internet activity.

Although the use of encryption provides additional privacy protections, it does not render BIAS providers blind to consumer preferences and online activity. Also, even though one study found that 42 of the top 50 Internet sites use encryption, 17 of those 42 only encrypt traffic after a user logs in. In fact, despite the increased use of encryption on the Internet today, more than half of enterprises do not extensively use encryption. Unlike BIAS providers that can see the

website destinations and other granular records related to Internet activity regardless of encryption, edge services (including those that use HTTPS) are limited to receiving data on websites where they are directly integrated. Among other things, this difference means that consumers can detect (and avoid) connections to particular edge providers using commercially available tools, something they cannot do with their BIAS provider.

Even though BIAS providers can choose to offer new edge services at any time, the reverse is not true. The BIAS market is characterized by higher market entry challenges and switching costs than the market for edge services. And whereas consumers can participate in limitless social media platforms, stream video from multiple sources, and engage with more than one e-mail service provider, they have no need for more than one paid BIAS plan per device.

The record also includes many comments encouraging the Commission to adopt a more flexible, fact-specific approach to data privacy and security, in line with the model used by the Federal Trade Commission ("FTC"). The FTC's approach to data privacy and security is bounded by terms such as "reasonable" (in the case of an alleged deceptive practice) and a need to consider the benefits to competition (in the case of an alleged unfair practice). This approach has protected consumers' online privacy interests for nearly two decades while allowing for competition and innovation, and the Commission should use the tools at its disposal to more closely align its Section 222 implementation with the FTC's model. It should also thoughtfully address other proposals from the FTC's Bureau of Consumer Protection staff, such as providing safe harbors for privacy policies and data security and clarifying the definition of a BIAS provider. Any safe harbor standards and disclosure requirements should be flexible so that they can remain relevant over time.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WT Docket No. 16-106
Broadband and Other Telecommunications	)	
Services	)	

REPLY COMMENTS OF THE INTERNET ASSOCIATION

I. INTRODUCTION.

The Internet Association[1] respectfully submits these reply comments in response to comments filed regarding the Commission's April 1, 2016 Notice of Proposed Rulemaking ("*NPRM*") in the above captioned-proceeding.[2] As discussed below, a diverse array of commenters agree that the Commission could not apply Section 222 of the Communications Act to providers of edge services. Moreover, contrary to what some commenters suggest, edge service providers do not have comprehensive visibility into online activity and consumer information transmitted across the Internet, and the Commission's proposed rules do nothing to

[1] The Internet Association represents the interests of America's leading Internet companies and their global community of users. It is dedicated to advancing public policy solutions that strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. It is also committed to protecting users' online privacy by providing cutting-edge tools that empower users to make choices about how they view content online. The Internet Association's members include Airbnb, Amazon, Coinbase, Doordash, Dropbox, eBay, Etsy, Expedia, Facebook, FanDuel, Google, Groupon, Handy, IAC, Intuit, LinkedIn, Lyft, Monster, Netflix, Pandora, PayPal, Pinterest, Practice Fusion, Rackspace, reddit, Salesforce.com, Snapchat, Spotify, SurveyMonkey, Ten-X, TransferWise, TripAdvisor, Turo, Twitter, Uber Technologies Inc., Yahoo!, Yelp, Zenefits, and Zynga.

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, FCC 16-39 (rel. Apr. 1, 2016) ("*NPRM*").

detract from competition on the Internet. At the same time, the record reflects that the FTC's flexible approach to data privacy and security enforcement can better protect consumers and encourage innovation than a host of prescriptive rules. The FCC should more closely align its Section 222 implementation with the FTC's model and should also thoughtfully address other proposals from the staff of the FTC's Bureau of Consumer Protection.

II. A DIVERSE ARRAY OF COMMENTERS SUPPORT THE COMMISSION'S PROPOSED FINDING THAT SECTION 222 DOES NOT APPLY TO PROVIDERS OF EDGE SERVICES AND OTHER NON-TITLE II OFFERINGS.

In the *NPRM*, the Commission proposes to apply its existing statutory authority "solely to the existing class of services that Congress included within the scope of Title II, namely the delivery of telecommunications services."[3] Many commenters – as varied as civil society organizations, academics, trade associations, and technology companies – all agree that the Commission properly excluded edge services from the proposed requirements and, in fact, could not apply Section 222 to these services. For example, they write:

- *[T]he Commission's authority to regulate communications does not extend to providers at the edge of networks, nor does CDT believe that it should.*[4]

  -The Center for Democracy and Technology

- *[B]roadband providers are clearly covered by the protections for those communicating over common carriers that is afforded by § 222, and the edge providers are not.*[5]

  -The American Civil Liberties Union

- *The NPRM correctly recognizes the distinction [between BIAS providers and edge providers] and the several reasons for this difference in treatment so we will not repeat*

[3] *Id.* ¶ 13; *see also* 47 U.S.C. § 153(51) (stating that Title II's common carrier requirements apply to telecommunications carriers "only to the extent that [they are] engaged in providing telecommunications services").

[4] Comments of the Center for Democracy & Technology, WT Docket No. 16-106, at 1 (filed May 27, 2016).

[5] Comments of the American Civil Liberties Union, WT Docket No. 16-106, at 3 (filed May 27, 2016).

them here, other than to repeat the obvious fact that registries and registrars are not providing a Title II service – which means § 222 cannot apply to their activities.[6]

-Internet Infrastructure Coalition

- *Regulatory oversight for privacy practices of edge services generally lies with the Federal Trade Commission rather than the FCC.*[7]

-Mozilla

- *The FCC does not have authority to impose privacy rules on edge providers under Title II.*[8]

-John Peha (Professor, Carnegie Mellon University)

- *[Collection of data by edge providers is] outside of the FCC's jurisdiction.*[9]

-Online Trust Alliance

- *At core, the Commission's limitation is a direct result of the conclusions it reached in developing the 2015 Open Internet Order.*[10]

-Computer and Communications Industry Association

- *The definition of BIAS as defined in the NPRM also makes clear that OTT services providers are not within the regulatory realm of the FCC.*[11]

-Information Technology Industry Council

Some commenters argue that the *NPRM* would create different regulatory environments between BIAS providers and edge providers (and may be implying that the proposed rules

[6] Comments of the Internet Infrastructure Coalition, WC Docket No. 16-106, at 2 (filed May 27, 2016).

[7] Comments of Mozilla, WC Docket No. 16-106, at 5 (filed May 27, 2016) ("Mozilla Comments").

[8] Comments of Jon Peha, WC Docket No. 16-106, at 2 (filed May 27, 2016).

[9] Comments of the Online Trust Alliance, WC Docket No. 16-106, at 2 (filed May 27, 2016).

[10] Comments of the Computer and Communications Industry Association, WC Docket No. 16-106, at 1 (filed May 27, 2016).

[11] Comments of the Information Technology Industry Council, WC Docket No. 16-106, at 6 (filed May 27, 2016).

should also apply to edge providers).[12] However, these commenters fail to identify either legal authority or a clear need for the FCC to extend any new requirements to edge service providers. Some also specifically point out that Section 222 is limited in scope and does not cover edge providers. For instance, CTIA states that Congress drafted Section 222 to protect certain information that carriers obtain solely by providing *voice* telephone services.[13] NCTA similarly argues that "the Commission lacks statutory authority to impose the proposed rules under Section 222 because that provision only applies to privacy in the telephony context."[14]

The record overwhelmingly supports the FCC's position that Section 222 cannot be applied to edge providers, and that no new requirements should be imposed on edge providers. Comments also affirm that, given the distinctions between BIAS providers and others in the Internet ecosystem (as discussed in Section III), the FCC correctly focused on BIAS providers in the *NPRM*.[15] Moreover, as the Internet Association discussed in its comments, new requirements on edge services are unnecessary.[16] The FTC currently exercises robust oversight of non-Title II services on privacy, security, and other consumer protection issues, as do state regulators. Adopting additional data privacy and security requirements on edge services and other non-Title II offerings would upend the current regulatory framework without providing meaningful additional benefits for consumers.

---

[12] *See, e.g.*, Comments of the Wireless Association, WC Docket No. 16-106, at 153-54 (filed May 26, 2016) ("CTIA Comments"); Comments of AT&T, WC Docket No. 16-106, at 55-56 (filed May 27 2016) ("AT&T Comments"); Comments of the National Cable & Telecommunications Association, WC Docket No. 16-106, at 55-56, 81 (filed May 27, 2016) ("NCTA Comments").

[13] *See* CTIA Comments at 23.

[14] *See* NCTA Comments at 2.

[15] *See e.g.*, Mozilla Comments.

[16] Comments of the Internet Association, WC Docket No. 16-106 (filed May 27, 2016).

III. EDGE PROVIDERS DO NOT HAVE THE SAME ACCESS TO CONSUMER INFORMATION AS BIAS PROVIDERS.

A. Edge Providers Have More Limited Visibility Into Online Practices And Consumer Information.

Contrary to what some commenters suggest, edge providers do not have access to more or a wider range of user information than BIAS providers.[17] Edge providers typically have access to information when consumers voluntarily choose to establish a relationship with them or provide such information, including for example when they choose to register with a website, use certain features, or contribute a post to an online forum. Many edge providers also offer granular privacy settings that provide consumers with significant control over personal information.[18] When edge providers offer websites or have features integrated in other companies' websites, their presence is visible using commonly available software, which allows consumers to choose not to allow information collection by a particular edge provider. For instance, users can browse in anonymous or "private" mode, clear web caches, and use their browser settings to prevent edge providers from reading or writing cookies on their computers. A consumer also can use browser plugins to see which edge providers are collecting data on a particular page, and to choose which connections the consumer wishes to allow.

In contrast, BIAS providers are the only parties in the online ecosystem that can potentially see across the entire "highway" of Internet traffic traveling across their network – all of a consumer's network traffic goes through that person's BIAS provider – and do so without code that is clearly detectable by consumers on the webpages they load. One way to understand this process is by looking at the network through the seven-layer Open Systems Interconnection

[17] *See e.g.*, Comments of Peter Swire, WC Docket No. 16-106, at 8 (filed May 24, 2016) ("Non-ISPs Often Have Access to More and a Wider Range of User Information than ISPs") ("Peter Swire Comments").

[18] Mozilla Comments at 5.

("OSI") model.[19] The lowest four layers – the physical layer, data link layer, packet networking layer, and transport layer – are what BIAS providers use to deliver their services. Edge providers, on the other hand, rely on the highest three layers of the model – the session layer, presentation layer, and application layer. To even access or connect with any individual edge services provider, a consumer must first progress through the lower layers of the OSI model delivered by a BIAS provider.[20] As Mozilla explains, a BIAS provider has significant potential visibility into a consumer's usage patterns and traffic metadata.[21] The FTC came to a similar conclusion in 2012, explaining that BIAS providers are "in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible" based on their unique position as a major gateway to the Internet.[22] BIAS providers may also be able to view financial data or other sensitive information that consumers enter online.[23]

[19] SANS Institute, *The OSI Model: An Overview*, https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543 (last accessed June 20, 2016).

[20] *See, e.g.*, *Comments* of the Consumer Federation of California, WC Docket No. 16-106, at 6 (filed May 27, 2016).

[21] Mozilla Comments at 4.

[22] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at 56 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("2012 FTC Privacy Report").

[23] Some commenters flagged as a potential concern BIAS providers' ability to engage in deep packet inspection, which allows BIAS providers the ability to analyze the data packets that traverse their networks. *See, e.g.*, Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106, at 20 (filed May 27, 2016) ("FTC Staff Comments").

Edge service providers can, at best, typically only view their own "lane" of traffic.[24] For instance, Internet company XYZ can view the activities of consumers of its website and mobile apps while consumers are using the website and apps and any websites and apps that choose to include functionality that XYZ provides, but XYZ cannot directly see the other Internet websites that those consumers view or the other apps or online services that they use. In contrast, a BIAS provider can see that its broadband customer has visited XYZ's website – as well as the other websites, apps, and online services that the customer accesses.

B. Encryption Provides Additional Privacy Protections But Does Not Negate BIAS Providers' Access to Consumer Data.

Some commenters argue that there is a rapid shift to encryption, which denies BIAS providers comprehensive visibility into user activity.[25] The Commission and commenters have correctly recognized, however, that the use of encryption, while helpful to improve the security of online activity, does not render all BIAS providers as somehow blind to consumer preferences and other data. Encrypted Internet traffic itself can be revealing, and thus the percentage of traffic that is encrypted is not a reliable indicator of the impact on consumer privacy. As discussed by the Commission, even when traffic is encrypted, a BIAS provider may have access to, *inter alia*, what websites a customer has visited, how long and during what hours of the day the customer visited various websites, the customer's location, and what mobile device the customer used to access those websites.[26]

---

[24] *See, e.g.*, Comments of the Electronic Frontier Foundation, WC Docket No. 16-106, at 1 (filed May 27, 2016) ("No edge provider enjoys the ability to see everything a consumer does online").

[25] *See e.g.*, Peter Swire Comments at 7; Letter from Jacquelyne Flemming, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed June 28, 2016).

[26] Mozilla Comments at 4; *NPRM* ¶ 4.

Technical experts have demonstrated that Internet service providers can learn a significant amount about the contents of encrypted traffic without breaking or weakening encryption.[27] For example, they can use the features of network traffic, such as the size, timing, and destination of encrypted packets, to "uniquely identify certain web page visits or otherwise obtain information about what the traffic contains."[28] Even when users browse over secure HTTPS connections, researchers have been able to successfully infer "the medical condition of users of a personal health web site, and the annual family income and investment choices of users of a leading financial web site," as well as to "reconstruct portions of encrypted VoIP conversations."[29]

Arguments that the majority of Internet traffic is encrypted also warrant additional attention. For instance, one commenter argued that 42 of the top 50 Internet sites use encryption.[30] However, of the 42 websites noted, 17 of them encrypt traffic only after a user logs in, and the data does not show what percent of users on each of those websites chooses to log in.[31] Recent estimates suggest that about 40 percent of enterprises use encryption extensively.[32]

In any case, statistics on encryption do not tell the whole story because revealing data is still visible to BIAS providers (as explained above). Unlike BIAS providers that can see the

[27] Upturn, *What ISPs Can See*, https://www.teamupturn.com/reports/2016/what-isps-can-see (last accessed June 20, 2016) ("Upturn Report").

[28] *Id*.

[29] *Id.*

[30] Peter Swire Comments at 25.

[31] *Id*. at 36-37.

[32] Maria Korolov, *Study: Encryption use increase largest in 11 years*, CSO (Feb. 2016), http://www.csoonline.com/article/3088916/data-protection/study-encryption-use-increase-largest-in-11-years.html.

website destinations and other activity regardless of encryption, edge services (including those that use HTTPS) may not be able to identify users until they are logged in.

C. Market Entry Challenges And Switching Costs May Limit BIAS Customers' Data Privacy And Security Choices.

Compared to edge services, the BIAS marketplace is characterized by stronger financial, technical, and legal challenges to entry for service providers, as well as substantial switching costs for consumers.

BIAS Market Entry Challenges. Telecommunications networks have high market entry costs. Whereas consumers can participate in limitless social media platforms, stream video from multiple sources, and engage with more than one e-mail service provider, they typically pay for only one BIAS plan per device.

New BIAS entrants may need to install facilities such as poles, dig trenches, lay conduit, locate and construct wireless antennas, or engage in other infrastructure deployment. These activities involve significant construction costs that require at least a minimum scale. New entrants also may need to obtain approval from local governments for access to publicly owned rights-of-way to allow them to place wires above or below property, and to locate their wireless facilities. Similarly, new entrants might need to contract with public utilities to rent space on utility poles or in underground spaces. At times, attempts by localities to create streamlined regulations to facilitate entry has been met by lawsuits by incumbents, which may frustrate competitive entry.[33] Thus, before even factoring in the costs of telecommunications equipment, facilities, electrical utilities, and hiring and training staff to provide marketing, billing, technical,

[33] *See, e.g., BellSouth Telecommunications, LLC v. Louisville/Jefferson County Metro Government*, No. 3:16-CV-00124-TBR (W.D. Ky.) and *Cox Communications Arizona LLC v. City of Tempe*, No. CV-15-01829-PHX-JJT (D. Ariz.).

and operational support, the financial resources and time needed to enter the BIAS marketplace are high by any measure.

An app developer and other edge providers, by contrast, need little more than a standard Internet-connected computer. Consumers can easily decide to use (or not use) any website or app, or can chose to use multiple edge providers (*i.e.*, "multihome") – and the robust state of competition online shows that they are doing just that.

BIAS Switching Costs. Switching edge services normally involves a few mouse clicks. Moreover, most of users' activity involves visiting websites that do not charge any fees. Users are not tied to these websites and can choose to pick a new online publication to read, search engine to use, or email provider with ease (including any edge services offered by BIAS providers).

The ease with which a consumer may explore various edge service offerings stands in contrast to the relatively higher switching costs between BIAS providers. To switch BIAS providers, a customer would need to first cancel the service agreement with their existing provider and then set up their new service (assuming a sufficient substitute is available). Not only is this typically a multi-step process that frequently involves phone calls and installation appointments, but there are also financial considerations. Customers may need to put down a new deposit and pay a set-up or installation fee to the new BIAS provider, and also may have to pay an early termination fee to the old provider. Of note, when broadband customers have been asked about the factors that might keep them from switching service, respondents with the choice of more than one provider have stated factors such as set up or installation fees, the process of

getting new service installed, putting down a new deposit, and having to change their current bundle of Internet, TV, and phone service.[34]

Competition and Privacy Choices. Some commenters suggest that the *NPRM* would reduce competition between BIAS providers that wish to undertake new edge services and edge providers that provide those services today, but this argument is a red herring.[35] As discussed below, the proposed restrictions on use of customer information would apply to covered information that "a BIAS provider acquires ***in connection to its provision of BIAS***."[36] If a BIAS provider wished to operate an edge service without using data that it collected in connection with its provision of BIAS – that is, on the same basis as edge providers – then the proposed rules would not restrict the BIAS provider from doing so. Accordingly, BIAS providers' edge services are implicated only if they choose to leverage data that they uniquely hold as BIAS providers in offering those services.

As discussed above, BIAS customers are required to provide metadata to BIAS providers, and those customers may not consider the potential disclosure of private information that can come from metadata.[37] Consumers may provide financial or other sensitive information online, and BIAS providers should not be able to leverage their unique access to this information in a way that favors their own payment services over those of unaffiliated edge service providers. The FCC noted differences in user control in the *NPRM*, stating that "edge providers only have direct access to the information that customers choose to share with them by virtue of engaging

---

[34] *See, e.g.*, Tom Wheeler, Chairman, Fed. Comm. Comm'n, Remarks at 1776 Headquarters (Sep. 4, 2014) (stating that "[o]nce consumers choose a broadband provider, they face high switching costs that include early-termination fees, and equipment rental fees").

[35] *See e.g.*, AT&T Comments at 55.

[36] *NPRM* Proposed Sec. 64.7000(f).

[37] Mozilla Comments at 4-5.

their services; in contrast, broadband providers have direct access to potentially all customer information, including such information that is not directed at the broadband provider itself to enable."[38]

IV. THE FTC'S FLEXIBLE APPROACH TO DATA PRIVACY AND SECURITY ENFORCEMENT CAN BETTER PROTECT CONSUMERS AND ENCOURAGE INNOVATION THAN A HOST OF PRESCRIPTIVE RULES.

Although the FCC's reclassification of BIAS under Title II removed BIAS offerings from the FTC's jurisdiction and created the need for the FCC to take action in this proceeding, the FCC has discretion over the implementation framework that it uses to protect BIAS customer data privacy and security. Many commenters in this proceeding agree that the FTC's approach is an effective framework for protecting consumer data privacy and security while also allowing for innovation and competition. Consistent with those filings, the FCC should consider adopting a similar model for its Section 222 implementation.

The FTC's approach is based on two standards – its prohibitions against "unfair" and "deceptive" acts or practices.[39] A misrepresentation or omission is "deceptive" if it is material and misleads or is likely to mislead consumers acting reasonably under the circumstances.[40] An act or practice is "unfair" if it causes, or is likely to cause, substantial injury to consumers that is not reasonably avoidable by consumers themselves, and that is not outweighed by countervailing

---

[38] *NPRM* ¶ 132.

[39] 15 U.S.C. § 45(a). The FTC also enforces a number of privacy statutes such as the Children's Online Privacy Protection Act (15 U.S.C. §§ 6501-6505) and the Fair Credit Reporting Act (15 USC § 1681 *et seq*.). However, outside of specific statutes passed by Congress, the FTC relies on its general unfair and deceptive acts and practices authority to carry out its work on privacy and data security.

[40] *See* FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf .

benefits to consumers or competition.[41]

The FTC has applied this flexible framework to the Internet ecosystem for nearly two decades, and it has protected the privacy interests that consumers value most while allowing for competition and innovation. The FTC's approach provides latitude to enforce information-handling practices while also tending to limit the agency's enforcement actions to more substantive cases of potential privacy violations. The FTC's approach, for instance, is meant to be bounded by terms such as "material" and "reasonable" (in the case of an alleged deceptive practice) and a need to consider the benefits to competition (in the case of an alleged unfair practice).

Another hallmark of the FTC's privacy framework is its flexible and considered approach. Rather than imposing a series of rigid, generally applicable data privacy and security rules for the Internet ecosystem, the FTC approaches privacy and security issues one case at a time, based on the specific facts of each alleged violation. This flexible approach to protecting consumer data privacy and security can often be preferable to prescriptive rules, especially for parts of the online ecosystem where technology advances daily.

Many commenters support the FTC's approach, calling it "successful",[42] "consumer-oriented,"[43] "flexible,"[44] and "time-tested."[45] Many have also requested that the FCC align its

---

[41] *See* FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness; 15 U.S.C. §45(n).

[42] Comments of the American Cable Association, WC Docket No. 16-106, at 39 (filed May 27, 2016).

[43] Comments of the Competitive Carriers Association, WC Docket No. 16-106, at 3 (filed May 27, 2016).

[44] *See e.g.*, AT&T Comments; CTIA Comments.

[45] Comments of the Consumer Technology Association, WC Docket No. 16-106, at 4 (filed May 27, 2016).

rules with the FTC's approach going forward.[46] As Chairman Wheeler has stated, the FTC has a "terrific model" and "thoughtful, rational approach."[47]

The *NPRM* did not closely follow the FTC's time-tested approach. For example, the *NPRM* proposes opt-in consent for many uses of customer personal information regardless of the potential for harm or the benefits to competition.[48] As FTC Commissioner Maureen Ohlhausen and FTC Bureau staff commented, this one-size-fits-all opt in approach does not reflect the different expectations and concerns that consumers have for data; as a result, the FCC's proposed rule could hamper beneficial uses of data that consumers may prefer.[49] Also, the *NPRM* arguably imposes strict liability on companies for failing to ensure security, another departure from the FTC's reasonableness standard for data security.[50] FTC Bureau staff suggests instead requiring BIAS providers to ensure *reasonable* security.[51] We agree that the FCC should clarify that data security liability considerations are based on whether companies have taken *reasonable* actions to protect the data. Any FCC requirements should recognize what security experts have said for decades – no network or device is 100 percent secure. Holding companies strictly liable

---

[46] *See e.g.*, AT&T Comments at 1.

[47] Margaret Harding McGill, *FCC, FTC Chiefs Zero In On Data Security, Privacy*, Law360, Jan. 6, 2016, http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-securityprivacy (*quoting* FCC Chairman Tom Wheeler).

[48] *NPRM* ¶¶ 107, 127-32.

[49] *See* FTC Staff Comments at 22; Statement of FTC Commissioner Maureen K. Ohlhausen Regarding Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106, at 1-3 (filed May 27, 2016).

[50] *Compare NPRM*, Proposed Rule 47 C.F.R. § 64.7005(a) *with* FTC, "Data Security," https://www.ftc.gov/datasecurity (last accessed June 20, 2016) ("The touchstone of the FTC's approach to data security is reasonableness: a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.").

[51] FTC Staff Comments at 27.

for data security creates the wrong incentives that could lead to wasteful use of resources, loss of functionality, barriers to the adoption of new technology, and other inefficiencies.

The FCC has multiple options to better align its practices with the FTC's flexible approach. For example, it can still choose to forbear from applying parts or all of Section 222 based on the newly developed record in this rulemaking proceeding (notwithstanding its earlier determination in the *2015 Open Internet Order*[52]). It can also implement Section 222 via flexible rules that track the FTC's Section 5 framework. In addition, it can use its enforcement discretion to ensure that it focuses on cases involving practices that materially harm consumers or where reasonable security practices are not followed. We encourage the Commission to use the tools at its disposal to ensure its BIAS rules more closely align with the FTC's model.

V. THE FCC SHOULD THOUGHTFULLY ADDRESS OTHER FTC BUREAU STAFF PROPOSALS

The FTC Bureau staff's comments provide additional useful guidance.[53] Below, we highlight and address key FTC staff recommendations that have not already been discussed in these reply comments.

Model Privacy Disclosures and Safe Harbor. The FTC Bureau staff proposed that the FCC develop a standardized "model" notice that would clearly communicate to consumers how their data is collected, used, and shared.[54] They also recommended that, to incentivize use of the model notice, the FCC provide a safe harbor, making clear that use of the model notice constitutes compliance with the *NPRM's* notice requirements.[55]

---

[52] *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5820-24 ¶¶ 456, 462-67 ("*2015 Open Internet Order*").

[53] *See* FTC Staff Comments.

[54] *Id.* at 13.

[55] *Id.* at 14.

We agree with this safe harbor proposal in concept, but we encourage the Commission to ensure that the model notice is not too rigid. For instance, the model notice should not specify the exact language that must be used but should instead include examples of the types of disclosures that would be appropriate. With changes in technology and practices, it would be difficult for the FCC to keep the model disclosure fully up to date. Consequently, any model privacy disclosure should allow enough flexibility to remain useful over time.

Data Security Safe Harbor. The FTC Bureau staff supported the development of data security safe harbors, but only if they include strong and concrete requirements backed by vigorous enforcement.[56] We agree that a data security safe harbor would be beneficial as long as the requirements are flexible enough to adapt to evolving security standards. Rigid data security requirements may become obsolete before new rules are even published.

Appropriate Limits on the Definition of BIAS Provider. The FTC Bureau staff recommends that the FCC's final rules incorporate a definition of "BIAS provider" that applies only "*to the extent that* [a person or entity] is engaged in the provision of BIAS."[57] Title II and its implementing rules apply to telecommunications carriers "only to the extent that [they are] engaged in providing telecommunications services."[58] The text of the *NPRM* suggests that a similar definition is intended here.[59] However, the limiting phrase "to the extent that" is not explicitly included in the proposed definition. We agree with the FTC's proposed clarification to ensure that the rule is not mistakenly applied to non-BIAS offerings.

---

[56] *Id.* at 29.

[57] *Id.* at 3, n.6.

[58] 47 U.S.C. § 153(51); *see also* 47 U.S.C. § 332(c)(1)(A), (c)(2)

[59] *See, e.g.*, *NPRM* ¶¶ 9, 11, 53-55.

VI. CONCLUSION.

The Commission should, consistent with the limits on its authority under the Communications Act, continue to exclude edge providers from any rules adopted in this proceeding and should adopt a more flexible FTC-style approach to its overall data privacy and security regulatory framework. The Commission also should thoughtfully consider the FTC Bureau staff's recommendations consistent with the points discussed above.

Respectfully submitted,

/s/ *Mark W. Brennan*

Abigail Slater
General Counsel
The Internet Association
1333 H Street NW
West Tower, Floor 12
Washington, DC 20005
(202) 770-0023

Mark W. Brennan
Partner
Hogan Lovells US LLP
555 13th Street, NW
Washington, DC 20004
(202) 637-6409

Counsel for The Internet Association

July 6, 2016